HAZVINEI NOMATTER MASIYA

Cybersecurity Professional | Security Operations | Detection Engineering | Automation

Harare, Zimbabwe | norman.masiya@gmail.com | +263 77 521 6823 / +263 71 866 2162

GitHub: https://github.com/hnmasiya | **Portfolio:** https://masiya-hub.org | **LinkedIn:** https://www.linkedin.com/in/hazvinei-masiya/

Global Resume · Remote · Hybrid · On-site · Relocation

PROFESSIONAL SUMMARY

CompTIA Security+ certified cybersecurity professional with 12+ years of enterprise IT experience spanning infrastructure, systems administration, network engineering, access control, endpoint security, and security-conscious technical operations. Hands-on cybersecurity work includes SIEM detection engineering, threat hunting, incident investigation, DFIR, Windows/Sysmon telemetry, network traffic analysis, and security automation using Wazuh, Sysmon, Python, Bash, and PowerShell. Employment experience and independent security-lab work are clearly distinguished.

GLOBAL RESUME APPLICATION PROFILE

Global / InternationalAfricaUK / EuropeNorth AmericaCanadaAustralia / New ZealandMiddle EastAsia-Pacific

This master resume uses internationally transferable terminology and ATS-friendly structure. Country-specific application versions can adjust only local conventions such as CV/resume terminology, work-authorization wording, address format, date style, and job-title wording—without changing or inventing career evidence.

CORE COMPETENCIES & TECHNICAL STACK

- **SIEM & Detection Engineering:** Wazuh SIEM, Sysmon XML Rules, Custom Alert Pipelines, FIM, MITRE ATT&CK mapping
- **DFIR & Threat Hunting:** Linux Auth/Syslog Forensics, PCAP Packet Analysis (Tshark/Wireshark), Hash Verification, evidence preservation and investigation workflows
- **Security Automation & Scripting:** Python, Bash, PowerShell, YAML, deterministic validation workflows
- **Enterprise IT & Systems Security:** Windows 10/11, Windows Server, Active Directory, Group Policy, Microsoft 365, RBAC, least privilege, endpoint hardening, patch management, authentication and access control
- **Network & Infrastructure Security:** LAN/WAN, Dell Versa SD-WAN, VOS, Cisco, Aruba, Sophos XG, network deployment, connectivity validation and infrastructure migration
- **Cloud & DevSecOps:** Azure Windows security lab, GCP Terraform architecture, GitHub Actions CI/CD, cloud security controls

SECURITY ENGINEERING PROJECTS & ARTIFACTS

Windows Sysmon / Wazuh LSASS Detection Validation

- Captured and validated Sysmon Event ID 10 telemetry from a self-owned Windows Server lab through Wazuh Agent 003 (dc01-lab).
- Correlated process access to `lsass.exe` with custom Wazuh detection logic, including observed event records and `GrantedAccess` values.
- Mapped the investigation to MITRE ATT&CK T1003.001 and T1059.001 while distinguishing observed LSASS access from proof of successful credential dumping.

Wazuh SIEM Rules & FIM Lab

- Authored custom XML detection rules for authentication and privilege-related activity and validated rule behavior against controlled test events.
- Configured File Integrity Monitoring across critical Linux system binaries and configuration files and documented validation methodology.

Linux Incident Response & DFIR

- Analyzed Linux authentication and system logs to reconstruct post-incident attack timelines.
- Verified SHA-256 evidence integrity and mapped unauthorized SSH activity to MITRE ATT&CK.

Active Directory Security Event Automation

- Developed Python tooling to parse Windows Security XML event logs (4624, 4625, 4728).

- Automated identification of suspicious authentication and privileged group-membership activity for investigation.

PCAP Traffic & Triage Automation

- Processed captured network traffic using Tshark and custom Python parsing scripts to identify suspicious HTTP requests, hosts, protocols, and indicators of compromise.
- Automated triage of web-application scanning and SQL-injection patterns in controlled laboratory traffic.

PROFESSIONAL EXPERIENCE

Jan 2025 – Present **Information Technology Support Specialist** | Netvantage Partners

- Deliver 1st and 2nd line technical support across client environments, resolving hardware, software, Windows endpoint, authentication, and connectivity issues.
- Support Active Directory accounts, user access, secure onboarding, structured patch management, and vulnerability mitigation across client systems.
- Investigate and escalate security-relevant incidents, including malware alerts and unauthorized access attempts, using security-aware triage.
- Develop IT support documentation and incident-handling procedures to standardize response consistency.

Jan 2021 – Present **IT Support Specialist (Contract & Consulting)** | Zuetech Technology Solutions

- Provide enterprise IT support, infrastructure administration, network operations, and onsite client deployment services across multiple environments.
- Administer Active Directory, RBAC, least-privilege access, Group Policy and Microsoft 365; troubleshoot authentication, endpoint and application issues.
- Monitor endpoint, network, and system activity for anomalies, applying security-aware triage principles to identify and escalate security-relevant incidents.
- Deploy and configure Dell Versa SD-WAN appliances, including VOS upgrades, IP configuration, migration support, and connectivity validation.
- Deliver endpoint protection, patch deployment, vulnerability mitigation, and technical documentation across client networks.
- Install and configure Yeastar P-Series PBX/UCaaS solutions for reseller clients as part of enterprise communications and infrastructure deployments.
- Client project — Network Infrastructure Upgrade, Mastercard Zimbabwe (Mar–Apr 2022): installed sensor LAN cabling, decommissioned legacy Cisco switches/controllers/APs, and racked/installed new Aruba controllers, switches, and access points.
- Client project — SD-WAN Circuit Deployment, SITA AERO (Jul 2026): configured two Dell Versa VEP1485 appliances via console CLI, connected each to dedicated internet circuits, and verified connectivity.
- Client project — Qatar Airways VOS Upgrade & SD-WAN Migration, Harare Airport Back Office & City Office (Aug 2026): performed VOS upgrading, device onboarding, and SD-WAN migration on Dell VEP1425 appliances.

Jan 2019 – Dec 2020 **Desktop Support Technician** | Raising Dawn Investment

- Administered user accounts, permissions, and security groups for 120+ users; supported access-control administration.
- Monitored Sophos Endpoint Protection and firewall telemetry, escalating security anomalies and endpoint issues.
- Supported backup, recovery, and business continuity operations, maintaining technical and operational documentation.

Jan 2016 – Dec 2018 **Information Technology Support Technician** | Compusys Technology

- Delivered desktop, network, and infrastructure support across multiple client environments; managed user access controls and permissions.
- Applied security patches, supported vulnerability remediation, and investigated authentication/access-control issues.
- Client project — IT Equipment Deployment and Configuration, Ericsson Zimbabwe (Nov 2016–Dec 2018): re-imaged laptop fleets, joined devices to the domain, configured email access, and installed network switches/access points.

Mar 2014 – Dec 2015 **Help Desk Support Technician** | shermanit

- Supported 200+ users across multiple business locations, providing remote and onsite technical support within defined SLA requirements.
- Troubleshot hardware, software, networking, and authentication issues; supported software deployments and infrastructure updates.
- Client project — IT Infrastructure Upgrade, AJP Group (May–Aug 2015): retired outdated systems, onboarded new devices to the domain, implemented VoIP phone systems, and migrated data to new systems.

Jul 2012 **IT System Migration and Setup (Contract)** | Abbeydale Group

- Engaged as outside technical support prior to formally joining shermanit: migrated servers, installed HP switches, re-imaged PCs, joined computers to the domain, connected VoIP phones, decommissioned outdated computers with

secure data disposal, and reconnected IP cameras to new PoE switches.

CYBERSECURITY VIRTUAL EXPERIENCE

Mastercard Cybersecurity Job Simulation — Forage | Completed September 20, 2026

- Designed a phishing email simulation and analyzed supplied phishing-campaign results to support security-awareness training.
- Created a phishing-awareness presentation covering phishing tactics, red flags, reporting and prevention.
- **Skills:** cybersecurity, security awareness, phishing analysis, security training, data analysis, data visualization, communication, problem solving and strategy.

Datacom Cyber Security Operations Job Simulation — Forage | Completed September 20, 2026

- Investigated a simulated cyberattack and documented findings, indicators, response priorities and security recommendations.
- Conducted a comprehensive cybersecurity risk assessment using a 5×5 likelihood/consequence approach across phishing, ransomware, third-party exposure, e-commerce/AWS and remote-access risks.
- **Skills:** information security, OSINT, research, risk assessment, risk management, security analysis, analytical skills and communication.

> Forage virtual job simulations; not employment with Mastercard or Datacom.

CERTIFICATIONS & EDUCATION

- **CompTIA Security+ (SY0-701)** — CompTIA
- **Google Cybersecurity Professional Certificate** — Google
- **Google IT Support Professional Certificate** — Google
- **BSc in Computer Science** — Unicaf University (In Progress)
- **Diploma in Information Technology** — Macmaine School of Computing
- **Diploma in PC Maintenance and Networking** — Macmaine School of Computing